Wartości $\left\{ {n \atop k} \right\}$ dla małych n i k:

n \ k	0	1	2	3	4	5	6	7	8	9
0	1	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0	0
3	0	1	3	1	0	0	0	0	0	0
4	0	1	7	6	1	0	0	0	0	0
5	0	1	15	25	10	1	0	0	0	0
6	0	1	31	90	65	15	1	0	0	0
7	0	1	63	301	350	140	21	1	0	0
8	0	1	127	966	1701	1050	266	28	1	0
9	0	1	255	3025	7770	6951	2646	462	36	1

Uwaga!

W przypadku, gdy $n \geqslant 0$ i $k < 0$ zakładamy, że $\left\{ {n \atop k} \right\} = 0$.

Potęgi kroczące

Definicja

Niech $m \geqslant 0$ będzie liczbą całkowitą.

- *Dolną silnią* nazywamy wyrażenie

$$x^{\underline{m}} = x(x-1)(x-2)\cdots(x-m+1).$$

- *Górną silnią* nazywamy wyrażenie

$$x^{\overline{m}} = x(x+1)(x+2)\cdots(x+m-1).$$

Wyrażenie $x^{\underline{m}}$ czytamy „x do m-tej ubywającej", a $x^{\overline{m}}$ — „x do m-tej przybywającej".

Twierdzenie

Dla $n > 0$ zachodzi zależność rekurencyjna

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \cdot \left\{ {n-1 \atop k} \right\}.$$

Dowód. *(1/2)*

Niech $S = \{a_1, a_2, \ldots, a_n\}$. Określimy liczbę podziałów S na k niepustych podzbiorów $S_1, S_2, \ldots, S_k$. Zauważmy, że w każdym takim podziale elementy $a_1, a_2, \ldots, a_{n-1}$ można przydzielić albo do zbiorów $S_1, S_2, \ldots, S_{k-1}$ albo do zbiorów $S_1, S_2, \ldots, S_{k-1}, S_k$ (w obu przypadkach każdy z wymienionych zbiorów posiada co najmniej jeden z elementów $a_1, \ldots, a_{n-1}$).

W pierwszym przypadku mamy $\left\{ {n-1 \atop k-1} \right\}$ możliwości. Zauważmy, że dla każdego takiego podziału element a_n tworzy jednoznaczenie jednoelementowy ostatni zbiór S_k: $S_k = \{a_n\}$.

Liczby Stirlinga drugiego rodzaju

Definicja

Podziałem skończonego zbioru S nazywamy rodzinę parami rozłącznych podzbiorów $\{S_1, S_2, \ldots, S_k\}$ zbioru S taką, że

$$S_1 \cup S_2 \cup \ldots \cup S_k = S.$$

Definicja (liczby Stirlinga drugiego rodzaju)

Symbol $\left\{ {n \atop k} \right\}$ (czyt. k podzbiorów n) oznacza liczbę sposobów podziału zbioru n-elementowego na k niepustych podzbiorów.

Liczby Stirlinga drugiego rodzaju występują częściej niż liczby Stirlinga pierwszego rodzaju, więc zaczynamy od nich — tak jak James Stirling w swojej książce *Methodus Differentialis* (1730).

Przykład

Wyznacz wartość $\left\{ {4 \atop 2} \right\}$.

Wyznaczymy liczbę podziałów zbioru czterolementowego $\{a, b, c, d\}$ na dwa niepuste zbiory. Zauważmy, że $4 = 1 + 3 = 2 + 2$, więc dany zbiór możemy zapisać jako sumę zbiorów trój- oraz jednoelementowego lub dwóch dwuelementowych:

$$\begin{aligned} 1+3: &\quad \{a\} \cup \{b,c,d\}, \quad \{b\} \cup \{c,d,e\}, \quad \{c\} \cup \{a,b,d\}, \quad \{d\} \cup \{a,b,c\}, \\ 2+2: &\quad \{a,b\} \cup \{c,d\}, \quad \{a,c\} \cup \{b,d\}, \quad \{a,d\} \cup \{b,c\}. \end{aligned}$$

Zatem $\left\{ {4 \atop 2} \right\} = 7$.

Dowód. *(2/2)*

Mamy

$$x^n = x \cdot x^{n-1} \overset{(ZI)}{=} x \cdot \sum_{k=0}^{n-1} \left\{ {n-1 \atop k} \right\} x^{\underline{k}} = \sum_{k=0}^{n-1} \left\{ {n-1 \atop k} \right\} x^{\underline{k}} \cdot x =$$

$$= \sum_{k=0}^{n-1} \left\{ {n-1 \atop k} \right\} (x^{\underline{k+1}} + kx^{\underline{k}}) = \sum_{k=0}^{n-1} \left\{ {n-1 \atop k} \right\} x^{\underline{k+1}} + \sum_{k=0}^{n-1} \left\{ {n-1 \atop k} \right\} kx^{\underline{k}} =$$

$$= 0 + \sum_{k=1}^{n} \left\{ {n-1 \atop k-1} \right\} x^{\underline{k}} + \sum_{k=0}^{n-1} \left\{ {n-1 \atop k} \right\} kx^{\underline{k}} + 0 =$$

$$= \left\{ {n-1 \atop -1} \right\} x^{\underline{0}} + \sum_{k=1}^{n} \left\{ {n-1 \atop k-1} \right\} x^{\underline{k}} + \sum_{k=0}^{n-1} \left\{ {n-1 \atop k} \right\} kx^{\underline{k}} + \left\{ {n-1 \atop n} \right\} nx^{\underline{n}} =$$

$$= \sum_{k=0}^{n} \left\{ {n-1 \atop k-1} \right\} x^{\underline{k}} + \sum_{k=0}^{n} \left\{ {n-1 \atop k} \right\} kx^{\underline{k}} = \sum_{k=0}^{n} \left(\left\{ {n-1 \atop k-1} \right\} + \left\{ {n-1 \atop k} \right\} k \right) \cdot x^{\underline{k}} =$$

$$= \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \cdot x^{\underline{k}}.$$

Wartości $\begin{bmatrix} n \\ k \end{bmatrix}$ dla małych wartości k:

- $k = 0$.

  Podobnie jak w przypadku liczb Stirlinga drugiego rodzaju mamy $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$ oraz $\begin{bmatrix} n \\ 0 \end{bmatrix} = 0$ dla $n > 0$.

- $k = 1$.

  Oczywiście $\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0$. Pamiętamy, że zbiór n-elementowy ma dokładnie $n!$ permutacji. Każdemu cyklowi odpowiada dokładnie n permutacji (każda rozpoczyna się od innego elementu danego zbioru), zatem

$$\begin{bmatrix} n \\ 1 \end{bmatrix} = \frac{n!}{n} = (n-1)!$$

Dowód. *(2/2)*

W drugim przypadku mamy $\left\{ {n-1 \atop k} \right\}$ możliwości podziału zbioru $\{a_1, a_2, \ldots, a_{k-1}\}$ na $S_1, S_2, \ldots, S_k$. Zauważmy, że w przypadku każdego takiego podziału element a_n może trafić do jednego z k zbiorów $S_1, S_2, \ldots, S_k$. Zatem w tym przypadku mamy $k \cdot \left\{ {n-1 \atop k} \right\}$ możliwości.

Ostatecznie

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \cdot \left\{ {n-1 \atop k} \right\}.$$

□

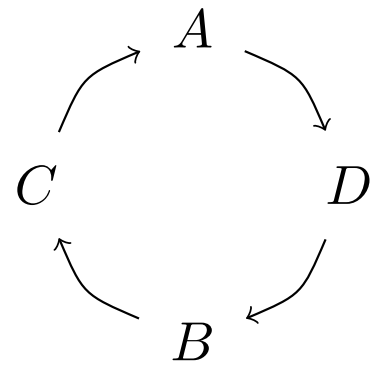
Liczby Stirlinga pierwszego rodzaju

Definicja

Cyklem nazywamy cykliczne ustawienia elementów danego zbioru.

Przykładowo jednym z cykli zbioru $\{A, B, C, D\}$ jest cykl w którym A przechodzi na D, D na B, B na C, a C na A. Ten cykl zapisujemy w postaci $[A, D, B, C]$. Oczywiście

$$[A, D, B, C] = [D, B, C, A] = [B, C, A, D] = [C, A, D, B].$$



Definicja (liczby Stirlinga pierwszego rodzaju)

Symbol $\begin{bmatrix} n \\ k \end{bmatrix}$ (czyt. k cykli n) oznacza liczbę sposobów na rozmieszczenie n elementów w k rozłącznych cyklach.

Liczby szczególne

dr inż. Bartłomiej Pawlik

19 czerwca 2024

Funkcja φ-Eulera

Definicja

Liczby całkowite a i b nazywamy **względnie pierwszymi**, gdy $\mathrm{NWD}(a, b) = 1$.

Zapis $a \perp b$ oznacza, że a i b są liczbami względnie pierwszymi.

Stwierdzenie

Liczby $\dfrac{a}{\mathrm{NWD}(a,b)}$ i $\dfrac{b}{\mathrm{NWD}(a,b)}$ są względnie pierwsze.

Przykład

$\mathrm{NWD}(48, 180) = 12$, więc 48 i 180 nie są liczbami względnie pierwszymi.

$$\frac{48}{12} = 4, \quad \frac{180}{12} = 15.$$

Zauważmy, że $\mathrm{NWD}(4, 15) = 1$. Zatem $4 \perp 15$.

Poprawność algorytmu Euklidesa

- Algorytm produkuje malejący ciąg liczb całkowitych nieujemnych $r_1 > r_2 > \ldots > r_n$ (jedna liczba w jednym kroku). Zatem algorytm zatrzymuje się po skończonej liczbie kroków (nie większej niż wartość r_1).
- Z własności $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - qb, b)$ otrzymujemy

$$\begin{aligned}\mathrm{NWD}(a, b) &= \mathrm{NWD}(b, r_1) = \mathrm{NWD}(r_1, r_2) = \ldots = \mathrm{NWD}(r_{n-1}, r_n) = \\ &= \mathrm{NWD}(r_n, 0) = r_n\end{aligned}$$

Definicja NWD

Niech $a, b \in \mathbb{Z}$ i niech co najmniej jedna z nich jest różna od 0. Liczbę naturalną d nazywamy **największym wspólnym dzielnikiem** liczb a i b, gdy

- $d|a$ i $d|b$,
- jeżeli dla $c \in \mathbb{N}$ mamy $c|a$ i $c|b$, to $c|d$.

Największy wspólny dzielnik liczb a i b oznaczamy jako $\mathrm{NWD}(a, b)$.

Przykład

$\mathrm{NWD}(6, 8) = 2, \quad \mathrm{NWD}(14, -17) = 1, \quad \mathrm{NWD}(-3, -9) = 3, \quad \mathrm{NWD}(0, 24) = 24.$

Stwierdzenie

Jeżeli $a \perp b$, to $\varphi(ab) = \varphi(a)\varphi(b)$.

Z dwóch ostatnich stwierdzeń wynika następujące

Twierdzenie

Niech $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ będzie postacią kanoniczną liczby $n \in \mathbb{N}/\{1\}$. Wtedy

$$\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Podstawowe twierdzenie arytmetyki

Każdą liczbę całkowitą dodatnią można przedstawić jako iloczyn liczb pierwszych. Przedstawienie takie jest jednoznaczne z dokładnością do kolejności czynników.

Przykład

$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$

Wniosek

Każda większa od 1 liczba naturalna n może być jednoznacznie zapisana w tzw. **postaci kanonicznej**

$$n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k},$$

gdzie q_i są liczbami pierwszymi, α_i są liczbami naturalnymi oraz $q_1 < q_2 < \ldots < q_k$.

Przykład

Postacią kanoniczną liczby 12 jest $2^2 \cdot 3$.

Elementy teorii liczb

dr inż. Bartłomiej Pawlik

23 kwietnia 2024

Współczynniki rozkładu silni

Twierdzenie

Niech n będzie liczbą całkowitą dodatnią i niech $\alpha_p(N)$ oznacza największą potęgę liczby p dzielącą liczbę N. Wtedy

$$\alpha_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Przykład

Wskaż największą potęgę liczby 3 dzieląca liczbę $100!$

Korzystając z powyższego wzoru mamy

$$\alpha_3(100!) = \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{9} \right\rfloor + \left\lfloor \frac{100}{27} \right\rfloor + \left\lfloor \frac{100}{81} \right\rfloor + \left\lfloor \frac{100}{243} \right\rfloor + \ldots =$$
$$= 33 + 11 + 3 + 1 + 0 + \ldots = 48.$$

Zatem szukana potęga to 3^{48}.

Stwierdzenie

Dla dowolnej liczby pierwszej p i liczby całkowitej dodatniej α zachodzi:

- $\varphi(p) = p - 1$,
- $\varphi(p^\alpha) = p^\alpha \cdot \left(1 - \frac{1}{p}\right)$.

Dowód.

- Liczba pierwsza p jest względnie pierwsza z każdą z liczb $1, 2, \ldots, p-1$.
- Zauważmy, że jedynie wielokrotności liczby pierwszej p mają wspólny nietrywialny dzielnik z p^α. Zatem w zbiorze $\{1, 2, \ldots, p^\alpha - 1\}$ liczbami niebędącymi liczbami względnie pierwszymi z p^α są

$$1 \cdot p,\ 2 \cdot p,\ \ldots,\ (p^{\alpha-1} - 1) \cdot p,$$

więc ich liczba wynosi $p^{\alpha-1} - 1$. Zatem

$$\varphi\left(p^\alpha\right) = \left(p^\alpha - 1\right) - \left(p^{\alpha-1} - 1\right) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

□

Definicja

Dla każdej liczby $n \in \mathbb{N}/\{1\}$ określamy liczbę $\varphi(n)$ jako liczbę dodatnich liczb całkowitych mniejszych od n i względnie pierwszych z n:

$$\varphi(n) = \Big|\{1 \leqslant k < n : \ k \perp n\}\Big|.$$

Funkcję $\varphi = \varphi(n)$ nazywamy **funkcją φ-Eulera**.

Przykład

Obliczmy NWD$(k, 12)$ dla k mniejszych od 12:

$$\begin{array}{llll} \text{NWD}(1,12) = 1, & \text{NWD}(4,12) = 4, & \text{NWD}(7,12) = 1, & \text{NWD}(10,12) = 2, \\ \text{NWD}(2,12) = 2, & \text{NWD}(5,12) = 1, & \text{NWD}(8,12) = 4, & \text{NWD}(11,12) = 1. \\ \text{NWD}(3,12) = 3, & \text{NWD}(6,12) = 6, & \text{NWD}(9,12) = 3, & \end{array}$$

Zatem

$$\varphi(12) = \Big|\{1,5,7,11\}\Big| = 4.$$

Własności NWD i NWW

Niech $a, b \in \mathbb{Z}/\{0\}$ i $q \in \mathbb{Z}$.

1. Jeżeli $a|b$, to $\mathrm{NWD}(a, b) = |a|$ i $\mathrm{NWW}(a, b) = |b|$.
2. $\mathrm{NWD}(a, b) = \mathrm{NWD}(|a|, |b|)$ i $\mathrm{NWW}(a, b) = \mathrm{NWW}(|a|, |b|)$.
3. $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - qb, b)$.
4. $\mathrm{NWD}(a, b) \cdot \mathrm{NWW}(a, b) = |a \cdot b|$.